WE CLAIM:

1. A communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising:

a key generating step of generating a secret key (p,q,β) satisfying

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

and

- $n = p^d q$ $(d > 1$ is odd.)
- k : binary length of pq
- $\alpha \in \mathbb{Z}$

a public key (n,k,α) satisfying

(1) an encrypting step performed by the sender device, of

;

$C = m^{2n\alpha} \bmod n$

computing

for plaintext m ($0 < m < 2^{k-2}$), computing Jacobi's symbol a=(m/n), and sending ciphertext (C,a) to the receiver device; and

(2) a decrypting step performed by the receiver device, of using the receiver's secret key (p,q,β) to compute

$$m_{1,p} = C^{\frac{(p+1)\beta_q - 1}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{(q+1)\beta_p - d}{4}} \bmod q$$

from the ciphertext (C,a), and regarding as the plaintext m any of $\phi(m_{1,p},m_{1,q})$, $\phi(-m_{1,p},m_{1,q})$, $\phi(m_{1,p},-m_{1,q})$, and $\phi(-m_{1,p},-m_{1,q})$ that satisfies (x/n)=a and $0<x<2^{k-2}$, where ϕ denotes ring isomorphism mapping from $Z/(p)\times Z/(q)$ to $Z/(pq)$ by the Chinese remainder theorem.

2. The communication method using public key cryptosystem according to Claim 1, comprising the step of:

generating and publicizing the public information (n,k,α) by the receiver device.

3. The communication method using public key cryptosystem according to Claim 1, wherein, for α=β=1, α and β are deleted from the public key and the secret key, respectively.

4. A communication system using public key cryptosystem in which a sender device encrypts send data by using a receiver's public key, the system comprising:

(a) a sender device comprising:

a key generating device for generating a secret key (p,q,β) satisfying

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

and

- $n = p^d q$ $(d > 1$ is odd$)$
- k : binary length of pq
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$

a public key (n,k,α,a) (k is the bit length of pq) satisfying

a device for computing

$C = m^{2n\alpha} \bmod n$

for plaintext m satisfying a=(m/n) ($0 < m < 2^{k-2}$) (a=(m/n denotes Jacobi's symbol); and

a communication device for sending ciphertext C to the receiver device; and

(b) a receiver device comprising:

$$m_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

a device using the receiver's secret key (p,q,β) to compute

from the ciphertext C; and

a device regarding as the plaintext m any of $\phi(m_{1,p},m_{1,q})$, $\phi(-m_{1,p},m_{1,q})$, $\phi(m_{1,p},-m_{1,q})$, and $\phi(-m_{1,p},-m_{1,q})$ that satisfies (x/n)=a and $0<x<2^{k-2}$, where ϕ denotes ring isomorphism mapping from $Z/(p)\times Z/(q)$ to Z/(pq) by the Chinese remainder theorem.

5. The communication system using public key cryptosystem according to Claim 4, wherein the receiver device comprises a device for creating the public information (n,k,α,a).

6. The communication system using public key cryptosystem according to Claim 4, wherein, for $\alpha=\beta=1$, α and β are deleted from the public key and the secret key, respectively.

7. The communication method using public key cryptosystem according to Claim 1, comprising the step of creating the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers.

8. The communication method using public key cryptosystem

according to Claim 1, comprising the step of creating the plain text m so as to include check information for checking whether message text to be sent to the receiver from the sender has been correctly decrypted.

9. The communication method using public key cryptosystem according to Claim 1, comprising the step of transforming message text to be sent to the receiver from the sender into plaintext m whose contents are provided with predetermined redundancy, and encrypting the plaintext m by the method described in Claims 1 or 4, wherein the receiver device decrypts the plaintext m by the method described in Claims 1 or 4 and checks the predetermined redundancy.

10. The communication method using public key cryptosystem according to Claim 1, comprising the step of transforming message text to be sent to the receiver from the sender into plaintext m whose contents are provided with a predetermined, meaningful message, and encrypting the plaintext m by the method described in Claims 1 or 4, wherein the receiver device decrypts the plaintext m by the method described in Claims 1 or 4 and checks the contents of the predetermined, meaningful message.

11. The communication method using public key cryptosystem according to Claim 1, wherein the value of d (d>1) is variable.

12. A key sharing method by which a sender device performs cipher communications by using a receiver's public key, the method comprising key generating steps of:

generating a secret key (p,q,β) satisfying

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

and

a public key (n,k,α) (k is the bit length of pq) satisfying

- $n = p^d q$ $(d > 1$ is odd$)$
- k : binary length of pq
- $\alpha \in \mathbb{Z}$
- f : one-way function ;

(1) in the sender device, to share a shared key K=f(m) with the

$C = m^{2n\alpha} \bmod n$

receiver device, for send data m ($0<m<2^{k-2}$), computing

and

computing Jacobi's symbol a=(m/n) and the shared key K by K=f(m), sending ciphertext (C,a) to the receiver device, and computing the shared key K=f(m); and

(2) in the receiver device, using the receiver's secret key (p,q,β) to compute

$$m_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

from the ciphertext (C,a), computing as the send data m any of $\phi(m_{1,p},m_{1,q})$, $\phi(-m_{1,p},m_{1,q})$, $\phi(m_{1,p},-m_{1,q})$, and $\phi(-m_{1,p},-m_{1,q})$ that satisfies (x/n)=a and $0<x<2^{k-2}$, where ϕ denotes ring isomorphism mapping from $Z/(p)\times Z/(q)$ to Z/(pq) by the Chinese remainder theorem, and computing the shared key K by K=f(m) using public information f.

13. The key sharing method according to Claim 12, comprising the step of:

generating and publicizing the public information (n,k,α) by the receiver device.

14. The key sharing method according to Claim 12, wherein, for $\alpha=\beta=1$, α and β are deleted from the public key and the secret key, respectively.

15. A key sharing method by which a sender device performs cipher communications by using a receiver's public key, the method comprising key generating steps of:

generating a secret key (p,q,β) satisfying

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

and

- $n = p^d q$ $(d > 1$ is odd$)$
- k : binary length of pq
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$
- f : one-way function

a public key (n,k,α,a) (k is the bit length of pq) satisfying

(1) in the sender device, to share a shared key K=f(m) with the receiver device, for send data m ($0<m<2^{k-2}$) satisfying a=(m/n) (a=(m/n) denotes Jacobi's symbol), computing

$C = m^{2n\alpha} \bmod n$

and

computing the shared key K by K=f(m), sending ciphertext C to the receiver device, and computing the shared key K=f(m); and

(2) in the receiver device, using the receiver's secret key (p,q,β) to compute

$$m_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

from the ciphertext C, computing as the send data m any of $\phi(m_{1,p},m_{1,q})$, $\phi(-m_{1,p},m_{1,q})$, $\phi(m_{1,p},-m_{1,q})$, and $\phi(-m_{1,p},-m_{1,q})$ that satisfies (x/n)=a and $0<x<2^{k-2}$, where ϕ denotes ring isomorphism mapping from Z/(p)×Z/(q) to Z/(pq) by the Chinese remainder theorem, and computing the shared key K by K=f(m) using public information f.

16. The key sharing method according to Claim 15, comprising the step of:

generating and publicizing the public information (n,k,α,a) by the receiver device.

17. The key sharing method according to Claim 15, comprising the step of, for α=β=1, deleting α and β from the public key and the secret key, respectively.

18. The key sharing method according to Claim 12, comprising the step of creating the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers.

19. The key sharing method according to Claim 12, wherein the value of d (d>1) is variable.

20. An encryption method in public key cryptosystem according to Claim 1, wherein one or more hash functions are publicized and the sender device comprises the steps of:

creating plaintext and random number information;

performing exclusive OR and data concatenation operations on the plaintext and the random number information;

Page 37 of 50

inputting results obtained by the operations to a relevant hash function and computing the input results;

performing exclusive OR and data concatenation operations on the plaintext, the random number information, and the results of input to the hash function; and

replacing the results of the operations in a location of the plaintext m in Claim 1 or the location of a random number r, and performing encryption according to the procedure of the public key cryptosystem in Claim 1.

21. A decryption method in public key cryptosystem, for decrypting ciphertext encrypted by the method set forth according to Claim 20, the method comprising:

the decrypting step set forth in Claim 1;

a step of restoring the plaintext m from the results of the logical OR and data concatenation operations performed in Claim 20;

a step of verifying the validity of the procedure of the (exclusive OR and data concatenation) operations; and

a step of outputting decryption results.

22. A communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret key (p,q,β) satisfying

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

and

a public key (n,k,k_0,k_1,α,G,H) satisfying

- $n = p^d q$ $(d > 1$ is odd$)$
- k, k_0, k_1 : k is a binary length of pq, and k_0, k_1 are positive integers with $k > k_0 - k_1 - 2$.
- $\alpha \in \mathbb{Z}$
- $G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0-2}$
- $H : \{0,1\}^{k-k_0-2} \to \{0,1\}^{k_0}$

$x = (m0^{k_1} \odot G(r))||(r \odot H(m0^{k_1} \odot G(r)))$

(1) in the sender device, computing

for plaintext m ($m \in \{0,1\}^l$, $l=k-k_0-k_1-2$) and a random number r($r \in \{0,1\}^{k0}$},

$C = x^{2n\alpha} \bmod n$

computing

and further computing Jacobi's symbol a=(x/n), and sending ciphertext (C,a) to the receiver device; and

(2) in the receiver device, using the receiver's secret key (p,q,β) to compute

$$x_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$
$$x_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

from the ciphertext (C,a), computing y that satisfies (y/n)=a and $0<y<2^{k-2}$ of $\phi(x_{1,p},x_{1,q})$, $\phi(-x_{1,p},x_{1,q})$, $\phi(x_{1,p},-x_{1,q})$, and $\phi(-x_{1,p},-x_{1,q})$, where ϕ denotes ring isomorphism mapping from Z/(p)×Z/(q) to Z/(pq) by the Chinese remainder theorem, further

when

$y = s||t$ $(s \in \{0,1\}^{k-k_0-2}, t \in \{0,1\}^{k_0})$

computing

$$z = G(H(s) \odot t) \odot s,$$

$$m = \begin{cases} [z]^l & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases},$$

and decrypting the plaintext m by

where $[a]^k$ and $[a]_k$ denote first k-bits and last k-bits of a, respectively.

23. The communication method using public key cryptosystem according to Claim 22, comprising the step of:

generating and publicizing the public information (n,k,k_0,k_1,α,G,H) by the receiver device.

24. The communication method using public key cryptosystem according to Claim 22, comprising the step of, for $\alpha=\beta=1$, deleting α and β from the public key and the secret key, respectively.

25. A communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$

key (p,q,β) satisfying

and

a public key (n,k,k_0,k_1,α,G,H) satisfying

- $n = p^d q$ $(d > 1$ is odd$)$
- $k, k_0, k_1 \in \mathbb{Z}$: k is a binary length of pq, and k_0, k_1 are positive integers with $k > k_0 - k_1 - 2$.
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$
- $G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0-2}$
- $H : \{0,1\}^{k-k_0-2} \to \{0,1\}^{k_0}$

(1) in the sender device, computing

$$x = (m0^{k_1} \odot G(r)) || (r \odot H(m0^{k_1} \odot G(r)))$$

that satisfies a=(x/n) for plaintext m ($m \in \{0,1\}^l$, $l=k-k_0-k_1-2$) and a random number r ($r \in \{0,1\}^{k_0}$) (a=(m/n) denotes Jacobi's symbol), computing

$$C = x^{2n\alpha} \bmod n$$

and further sending ciphertext C to the receiver device; and

(2) in the receiver device, using the receiver's secret key (p,q,β) to

$$x_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$
$$x_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

compute

from the ciphertext C, computing y that satisfies (y/n)=a and $0<y<2^{k-2}$ of $\phi(x_{1,p},x_{1,q})$, $\phi(-x_{1,p},x_{1,q})$, $\phi(x_{1,p},-x_{1,q})$, and $\phi(-x_{1,p},-x_{1,q})$, where ϕ denotes ring isomorphism mapping from Z/(p)×Z/(q) to Z/(pq) by the Chinese remainder theorem, further

when

$$y = s||t \quad (s \in \{0,1\}^{k-k_0-2},\ t \in \{0,1\}^{k_0})$$

$$z = G(H(s) \odot t) \odot s,$$

computing

$$m = \begin{cases} [z]^l & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{“reject”} & \text{otherwise} \end{cases}$$

and decrypting the plaintext m by

where $[a]^k$ and $[a]_k$ denote first k-bits and last k-bits of a, respectively.

26. The communication method using public key cryptosystem according to Claim 25, comprising the step of:

generating and publicizing the public information $(n,k,k_0,k_1,\alpha,a,G,H)$ by the receiver device.

27. A communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret key (p,q,β) satisfying

- $p,\ q$: prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1,q-1)}$

and

a public key (n,k,k_0,k_1,α,G,H) satisfying

- $n = p^d q$ $(d > 1$ is odd)
- $k, k_0, k_1 \in \mathbb{Z}$: k is a binary length of pq, and k_0, k_1 are positive integers with $k > k_0 - k_1 - 2$.
- $\alpha \in \mathbb{Z}$
- $G : \{0,1\}^{k_0} \rightarrow \{0,1\}^{k-k_0-2}$
- $H : \{0,1\}^{k-k_0-2} \rightarrow \{0,1\}^{k_0}$

$x = (m0^{k_1} \odot G(r))||(r \odot H(m0^{k_1} \odot G(r)))$

(1) in the sender device, computing

for plaintext m ($m \in \{0,1\}^l$, $l = k\text{-}k_0\text{-}k_1\text{-}2$) and a random number r($r \in \{0,1\}^{k0}$),

$C = x^{2n\alpha} \bmod n$

computing

and sending ciphertext C to the receiver device; and

(2) in the receiver device, using the receiver's secret key (p,q,β) to compute

$$x_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$
$$x_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

from the ciphertext C, for $y_1=\phi(x_{1,p},x_{1,q})$, $y_2=\phi(\text{-}x_{1,p},x_{1,q})$, $y_3=\phi(x_{1,p},\text{-}x_{1,q})$, and $y_4=\phi(\text{-}x_{1,p},\text{-}x_{1,q})$, where ϕ denotes ring isomorphism mapping from $Z/(p)\times Z/(q)$ to $Z/(pq)$ by the Chinese remainder theorem,

$y_i = s_i||t_i$ $(s_i \in \{0,1\}^{k-k_0-2}, t_i \in \{0,1\}^{k_0}, 1 \le i \le 4)$

when

computing

$$z_i = G(H(s_i) \odot t_i) \odot s_i \quad (1 \le i \le 4),$$

$$m = \begin{cases} [z_i]^l & \text{if } [z_i]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

and decrypting the plaintext m by

where $[a]^k$ and $[a]_k$ denote first k-bits and last k-bits of a, respectively.

28. The communication method using public key cryptosystem according to Claim 27, comprising the step of:

generating and publicizing the public information (n,k,k_0,k_1,α,G,H) by the receiver device.

29. The communication method using public key cryptosystem according to Claim 22, comprising the step of, for $\alpha=\beta=1$, deleting α and β from the public key and the secret key, respectively.

30. The communication method using public key cryptosystem according to Claim 22, comprising the step of creating the secret keys p and q by $p=2p'+1$ and $q=2q'+1$, where p' and q' are prime integers.

31. The communication method using public key cryptosystem according to Claim 22, wherein the value of d ($d>1$) is variable.

32. An encryption method according to Claim 1, for computing ciphertext C in two different devices, comprising the steps of:

$$C_1 = m^{2\alpha} \bmod n$$

in a device 1, after computing

outputting C_1 to a device 2; and

$C = C_1^n \bmod n$
in the device 2, by computing

computing the ciphertext C.

33. An encryption method according to Claim 22, for computing ciphertext C in two different devices, comprising the steps of:

$x = (m0^{k_1} \odot G(r)) || (r \odot H(m0^{k_1} \odot G(r)))$
in a device 1, computing

for plaintext m ($m \in \{0,1\}^l$, $l = k\text{-}k_0\text{-}k_1\text{-}2$) and a random number r($r \in \{0,1\}^{k0}$),

$C_1 = x^{2\alpha} \bmod n$
and after further computing

outputting C_1 to a device 2; and
in the device 2, by computing
$C = C_1^n \bmod n$

computing the ciphertext C.

34. A communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret

- p_i : prime integers ($p_i \equiv 3 \pmod 4$, $1 \leq i \leq h$)
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

key (p_i,β) ($1 \leqq i \leqq h$) satisfying

and

a public key (n,k,k_0,k_1,α,G,H) satisfying

- $n = \prod_{i=1}^{h} p_i$
- $k, k_0, k_1 \in \mathbb{Z}$: k is a binary length of pq, and k_0, k_1 are positive integers with $k > k_0 - k_1 - 2$.
- $\alpha \in \mathbb{Z}$
- $G : \{0,1\}^{k_0} \rightarrow \{0,1\}^{k-k_0}$
- $H : \{0,1\}^{k-k_0} \rightarrow \{0,1\}^{k_0}$

$x = (m0^{k_1} \odot G(r))||(r \odot H(m0^{k_1} \odot G(r)))$

(1) in the sender device, computing

for plaintext m (m∈$\{0,1\}^l$,l=k-k_0-k_1) and a random number r(r∈$\{0,1\}^{k0}$},

$C = x^{2\alpha} \bmod n$

computing

and sending ciphertext C to the receiver device; and

(2) in the receiver device, using the receiver's secret key (p_i,β) (1≦

$x_i = C^{\frac{(p_i+1)\beta}{4}} \bmod p_i$

i≦h) to compute

from the ciphertext C, for 2^h pieces of $\{\phi(e_1x_1,e_2x_2,...,e_hx_h) \mid e_1,...,e_h \in \{-1,1\}\}$ when

$y_i = s_i||t_i \quad (s_i \in \{0,1\}^{k-k_0},\ t_i \in \{0,1\}^{k_0},\ 1 \le i \le 2^h)$

computing

$$z_i = G(H(s_i) \odot t_i) \odot s_i \quad (1 \le i \le 2^h)$$

$$m = \begin{cases} [z_i]^{l} & \text{if } [z_i]_{k_1} = 0^{k_1} \\ \text{“reject”} & \text{otherwise} \end{cases},$$

and decrypting the plaintext m by

where ϕ denotes ring isomorphism mapping from Z/(p)×Z/(q) to Z/(pq) by the Chinese remainder theorem, and $[a]^k$ and $[a]_k$ denote first k-bits and last k-bits of a, respectively.

35. The communication method using public key cryptosystem according to Claim 34, comprising the step of:

generating and publicizing the public information (n,k,k_0,k_1,α,G,H) by the receiver device.

36. The communication method using public key cryptosystem according to Claim 34, for $\alpha=\beta=1$, deleting α and β from the public key and the secret key, respectively.

37. The communication method using public key cryptosystem according to Claim 34, comprising the step of:

sending the plaintext or the identification information of x along with ciphertext, or creating the plaintext m or x from publicized identification information.

38. The communication method using public key cryptosystem according to Claim 37, comprising the step of:

decrypting the plaintext m or the x from the ciphertext using the identification information sent along with the ciphertext or the publicized identification information.

39. The communication method using public key cryptosystem according to Claim 1, comprising the step of:

creating ciphertext C by

$C = m^{2\alpha} \bmod n$,

$m_{1,p} = C^{\frac{(p+1)\beta}{4}} \bmod p,$

$m_{1,q} = C^{\frac{(q+1)\beta}{4}} \bmod q$.

and creating $m_{1,p}$ and $m_{1,q}$ by

40. The communication method using public key cryptosystem according to Claim 22, comprising the step of:

creating ciphertext C by

$C = x^{2\alpha} \bmod n$,

$m_{1,p} = C^{\frac{(p+1)\beta}{4}} \bmod p,$

$m_{1,q} = C^{\frac{(q+1)\beta}{4}} \bmod q$.

and creating $m_{1,p}$ and $m_{1,q}$ by

41. A program product, comprising:

a program for instructing a computer to execute one of the key generating step, the encrypting step, and the decrypting step which are described in Claim 1; and

a medium embodying the program.

42. A communication system using public key cryptosystem which comprises a sender device and a receiver device and in which the sender device encrypts send data using a receiver's public key,

wherein the receiver device, using an operation unit the receiver

device has, executes the key generating step described in Claim 1 and generates the secret key (p,q,β) and the public key (n,k,α),

wherein the sender device, using an operation unit the sender device has, executes the encrypting step described in Claim 1, computes Jacobi's symbol a=(m/n), and sends ciphertext (C,a) to the receiver device, and

wherein the receiver device, using the operation unit the receiver device has, executes the decrypting step described in Claim 1 and obtains plaintext m.

43. The communication system using public key cryptosystem according to Claim 4, wherein the receiver device comprises a device that generates the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers.

44. The communication system using public key cryptosystem according to Claim 4, wherein the sender device comprises a device that generates the plaintext m so as to include check information for checking whether message text to be sent to the receiver has been correctly decrypted.

45. The communication system using public key cryptosystem according to Claim 4,

wherein the device of the sender device to encrypt the plaintext m provides predetermined redundancy to the message text to be sent to the receiver and produces the contents of the resulting message text as the plaintext m, and

wherein the device of the receiver device to decrypt the plaintext m checks the predetermined redundancy.

46. The communication system using public key cryptosystem

according to Claim 4,

wherein the sender device comprises the step of providing a predetermined, meaningful message to the message text to be sent to the receiver and producing the contents of the resulting message text as the plaintext m, and encrypting the plaintext m by the method described in Claim 4, and

wherein the receiver device comprises the step of decrypting the plaintext m by the method described in Claim 4, and checking the contents of the predetermined, meaningful message.

47. The communication system using public key cryptosystem in Claim 4, wherein the value of d ($d>1$) is variable.

09828213.040501